Научная статья
УДК 341.3
DOI: 10.37399/2686-9241.2025.3.179-192

Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве: анализ статьи 51 Устава ООН и перспективы самообороны в киберпространстве

Константин Константинович Лазарь
Дипломатическая академия МИД России, Москва, Российская Федерация
lazariconstantin@yandex.ru, https://orcid.org/0009-0008-4763-1922

Аннотация
Введение. В современном мире кибератаки становятся все более серьезной угрозой международной безопасности, способной причинять значительный ущерб государствам, нарушая критически важную инфраструктуру и подрывая национальную безопасность. Однако международное право до сих пор не дает однозначного ответа на вопрос о том, могут ли кибератаки квалифицироваться как «применение силы» или «акт агрессии» в контексте Устава ООН, что создает правовые пробелы и затрудняет применение права на самооборону. Поэтому целью исследования заявлены анализ международно-правовых норм и практик, связанных с квалификацией кибератак, а также рассмотрение перспектив развития международного права в области самообороны в киберпространстве. Ставятся задачи изучить понятие «применение силы» в международном праве применительно к кибератакам; рассмотреть возможность квалификации кибератак как «акта агрессии»; проанализировать применение права на самооборону в свете ст. 51 Устава ООН; выявить политико-правовые и доктринальные споры по данной тематике; оценить перспективы кодификации и унификации норм в области кибербезопасности.
Теоретические основы. Методы. Исследование опирается на нормы jus ad bellum Устава ООН (ст. 2(4), 51) и доктрину их применения к киберпространству в следующей логике: квалификация кибероперации определяется не способом, а масштабом и последствиями (физический вред, жертвы, долговременная утрата функциональности критической инфраструктуры, системный экономический ущерб). В этом аспекте различаются действия ниже порога силы, применение силы и вооруженное нападение; порог оценивается по интенсивности, длительности и совокупным эффектам. Кейс Stuxnet демонстрирует возможность материального ущерба киберсредствами. Выбор режима ответа зависит от атрибуции: самооборона требует вооруженного нападения и надлежащей атрибуции, тогда как контрмеры допустимы ниже порога силы при необходи-

мости, пропорциональности и обратимости. Подходы государств расходятся (США/Великобритания – адаптация действующих норм; Россия/Китай – акцент на киберсуверенитете и развитии специальных правил). МГП применяется при наличии вооруженного конфликта и задаёт критерии ratione materiae/temporis. Используется качественный метод исследования, включающий доктринальный анализ правовых норм и сравнительный подход к изучению позиций различных государств (Россия, США, Китай) и международных организаций по вопросам киберсуверенитета и самообороны.
Результаты исследования. Установлено, что кибератаки могут квалифицироваться как «применение силы» или «акт агрессии» при наличии существенного ущерба, сопоставимого с последствиями традиционного вооруженного нападения. Однако отсутствие четких международных норм и различия в позициях государств создают трудности в применении права на самооборону в киберпространстве.
Обсуждение и заключение. Необходима адаптация международного права к реалиям цифровой эпохи путем разработки новых международных норм и механизмов, учитывающих специфику киберпространства. Международное сотрудничество и диалог между государствами являются критическими для создания эффективной системы противодействия киберугрозам и обеспечения безопасности в цифровую эпоху.

Ключевые слова: кибератака, международное право, применение силы, акт агрессии, самооборона, Устав ООН, кибербезопасность

Для цитирования: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве: анализ статьи 51 Устава ООН и перспективы самообороны в киберпространстве // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192. DOI: 10.37399/2686-9241.2025.3.179-192.

Original article

Qualification of Cyberattacks as “Use of Force” or “Act of Aggression” in International Law: Analysis of Article 51 of the UN Charter and Perspectives of Self-Defense in Cyberspace

Constantin C. Lazari

Diplomatic Academy of the Ministry of Foreign Affairs of Russia, Moscow, Russian Federation
lazariconstantin@yandex.ru, https://orcid.org/0009-0008-4763-1922

Abstract
Introduction. In the modern world, cyberattacks have become a significant threat to international security, capable of causing substantial harm to states by disrupting critical infrastructure and undermining national security. However, international law does not yet provide a definitive answer on whether cyberattacks can be qualified as “use of force” or an “act of aggression” under the UN Charter, creating legal gaps and complicating the application of the right to self-defense. Purpose of the study is to analyze in-

ternational legal norms and practices related to the qualification of cyberattacks and to consider prospects for the development of international law in the field of self-defense in cyberspace. Tasks: to study the concept of “use of force” in international law as applied to cyberattacks; to consider the possibility of qualifying cyberattacks as an “act of aggression”; to analyze the application of the right to self-defense in light of Art. 51 of the UN Charter; to identify political-legal and doctrinal disputes on this topic; to assess the prospects for codification and unification of norms in the field of cybersecurity.
Theoretical Basis. Methods. The article relies on jus ad bellum under the UN Charter (Arts. 2(4), 51) and an instrument-neutral, scale-and-effects reading for cyberspace: qualification turns on magnitude and consequences (physical harm, casualties, long-term loss of critical infrastructure functionality, systemic economic impact) rather than means. This framework distinguishes below-force measures, use of force, and armed attack; thresholds are assessed via intensity, duration, and aggregate effects. Stuxnet illustrates material damage by cyber means. Response regimes hinge on attribution: self-defence presupposes an armed attack attributable to a state, whereas countermeasures address wrongful acts below the force threshold, subject to necessity, proportionality, and reversibility. State approaches diverge (US/UK – adapt existing law; Russia/China – emphasize cyber-sovereignty and tailored norms). IHL applies where operations occur in armed conflict, informing ratione materiae/temporis analysis.
A qualitative research method is used, including doctrinal analysis of legal norms and a comparative approach to studying the positions of various states (Russia, USA, China) and international organizations on issues of cyber sovereignty and self-defense.
Results. It has been established that cyberattacks can be qualified as “use of force” or an “act of aggression” when there is significant damage comparable to the consequences of a traditional armed attack. However, the absence of clear international norms and differences in state positions create difficulties in applying the right to self-defense in cyberspace.
Discussion and Conclusion. There is a need to adapt international law to the realities of the digital age by developing new international norms and mechanisms that take into account the specifics of cyberspace. International cooperation and dialogue among states are critical for creating an effective system to counter cyber threats and ensure security in the digital era.

Keywords: cyberattack, international law, use of force, act of aggression, self-defense, UN Charter, cybersecurity

For citation: Lazari, C. C. Qualification of cyberattacks as “use of force” or “act of aggression” in international law: analysis of article 51 of the un charter and perspectives of self-defense in cyberspace. *Pravosudie/Justice*. 2025;7(3):179-192. (In Russ.) DOI: 10.37399/2686-9241.2025.3.179-192.

Введение

В современном мире кибератаки стали неотъемлемой частью международной системы безопасности. Они способны причинять значительный ущерб, нарушая работу критически важной инфраструктуры, подрывая экономику и создавая угрозы национальной безопасности государств. Несмотря на рост числа подобных инцидентов, международное право до сих пор не дает однозначного ответа на вопрос о том, могут ли кибератаки квалифицироваться как «применение силы» или «акт агрессии» в контексте Устава ООН.

Статья 2(4) Устава ООН[1] запрещает государствам применять силу против территориальной целостности или политической независимости любого государства, за исключением случаев, предусмотренных самим Уставом. Статья 51 Устава предоставляет право на индивидуальную или коллективную самооборону в случае вооруженного нападения. Однако эти положения были разработаны в эпоху, когда угрозы исходили преимущественно от традиционных вооруженных конфликтов и не учитывали специфики киберпространства.

В свете этих обстоятельств возникает необходимость детального анализа правовых критериев, на основании которых кибератаки могут быть квалифицированы как «применение силы» или «акт агрессии» согласно ст. 51 Устава ООН. Также важно изучить механизмы адаптации международных норм для защиты государств в условиях кибератак и применения права на самооборону.

Цель исследования заключается в анализе существующих международно-правовых норм и практик, связанных с квалификацией кибератак, а также в рассмотрении перспектив развития международного права в этой области. Особое внимание уделяется тому, как международное сообщество может адаптировать действующие правовые механизмы для эффективного противодействия киберугрозам и обеспечения безопасности государств в цифровую эпоху.

В данной статье используется качественный метод исследования, включающий доктринальный анализ и сравнительный подход. Доктринальный анализ сосредоточен на изучении правовых норм, таких как Устав ООН и решения Международного Суда ООН. Сравнительный подход позволяет сопоставить стратегии и позиции различных государств (Россия, США, Китай) по вопросам киберсуверенитета и самообороны.

Также рассматривается деятельность международных организаций, таких как ООН и НАТО, с целью выявления правовых пробелов и оценки перспектив создания международно-правовых механизмов в сфере кибербезопасности.

Теоретические основы. Методы

Понятие «применение силы» в международном праве

Статья 2(4) Устава ООН четко запрещает применение силы в международных отношениях, кроме случаев самообороны или действий, санкционированных Советом Безопасности ООН. Однако термин «применение силы» в контексте кибератак остается недостаточно определенным. Согласно «Таллиннскому руководству 2.0»[2] применение силы в киберпространстве следу-

---

[1] Устав Организации Объединенных Наций. Подписан в Сан-Франциско 26 июня 1945 г., вступил в силу 24 окт. 1945 г. URL: https://www.un.org/ru/about-us/uncharter/full-text.

[2] *Jensen E. T.* The Tallinn Manual 2.0: Highlights and Insights // Georgetown Journal of International Law. 2017. Vol. 48, no. 3. P. 735–778. URL: https://

ет оценивать по последствиям, аналогичным традиционным вооруженным атакам [1]. Это означает, что кибератака может считаться применением силы, если она приводит к физическому ущербу, человеческим жертвам или значительным разрушениям инфраструктуры [2].

Для квалификации кибератаки как применения силы необходимо учитывать ее реальные последствия. Ярким примером является кибератака Stuxnet в 2010 г., которая привела к физическому повреждению иранских ядерных центрифуг [3]. Данное событие демонстрирует, что кибератака способна причинить ущерб, сопоставимый с традиционными военными действиями, и, следовательно, может рассматриваться как применение силы в соответствии с международным правом.

Резолюция 3314 (XXIX) Генеральной Ассамблеи ООН[3] определяет агрессию как вооруженное нападение на суверенитет, территориальную целостность или политическую независимость другого государства. Хотя в этой Резолюции не упоминаются кибератаки, по аналогии с традиционными формами агрессии можно предположить, что серьезные кибератаки могут квалифицироваться как акты агрессии, если они наносят значительный ущерб государству.

Соединенные Штаты Америки рассматривают кибератаки[4] на критическую инфраструктуру как потенциальное основание для применения права на самооборону [4]. В свою очередь, Россия и Китай, продвигая концепцию киберсуверенитета, утверждают, что любые кибератаки, нарушающие суверенитет государства, могут рассматриваться как агрессия, даже если они не приводят к физическому ущербу [5; 6].

Методы исследования

Анализ правовых норм базируется на изучении доктринальных источников и материалов международных организаций (ООН, НАТО). Сравнительный подход позволяет сопоставить национальные стратегии (Россия, США, Китай) применительно к квалификации кибератак и их правовых последствий. В рамках качественного метода рассмотрены также решения судов и официальные заявления государств, раскрывающие позиции относительно права на самооборону в киберпространстве. Такой комплексный подход помогает выявить пробелы в международном праве и определить направления возможной кодификации.

---

www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

[3] Резолюция Генеральной Ассамблеи ООН 3314 (XXIX) «Определение агрессии». Принята 14 декабря 1974 г. Документ ООН A/RES/3314 (XXIX). Нью-Йорк : ООН, 1974. URL: https://undocs.org/ru/A/RES/3314(XXIX).

[4] National Cyber Strategy of the United States of America (Национальная киберстратегия Соединенных Штатов Америки). Washington (DC) : The White House, September 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Результаты исследования

Возможность квалификации кибератаки как «акта агрессии»

Агрессия традиционно ассоциируется с физическими вооруженными действиями. Однако в условиях современного мира кибератаки способны причинять сопоставимый ущерб без непосредственного применения физической силы [7; 8]. Для того чтобы кибератака была квалифицирована как акт агрессии, необходимо оценить масштаб и характер причиненного ущерба.

Критериями могут служить разрушение критически важной инфраструктуры, серьезный экономический ущерб или массовые человеческие жертвы [9]. Например, кибератаки США против Ирана в 2019 г., направленные на системы управления и военные инфраструктуры[5], демонстрируют, как кибероперации могут использоваться в качестве средства агрессии[6].

Различные государства по-разному интерпретируют кибератаки. Соединенные Штаты и их союзники склонны считать серьезные кибератаки актами агрессии, оправдывающими применение права на самооборону [4]. В то же время Россия и Китай акцентируют внимание на защите суверенитета и выступают против широкого применения силы в ответ на кибератаки, особенно если нет явных доказательств и установленной атрибуции [10; 6].

«Таллиннское руководство 2.0» предлагает рассматривать кибератаки как вооруженные нападения, если их последствия эквивалентны традиционному применению силы. Однако отсутствие консенсуса среди государств и недостаточная кодификация данных норм усложняют их применение на практике [11; 12].

Право на самооборону в свете ст. 51 Устава ООН

Статья 51 Устава ООН предоставляет государствам право на индивидуальную или коллективную самооборону в случае вооруженного нападения. Применительно к кибератакам возникает вопрос: могут ли они считаться достаточным основанием для использования этого права?

Для применения права на самооборону в ответ на кибератаку должны быть выполнены определенные условия [13]. Во-первых, кибератака должна квалифицироваться как вооруженное нападение, т. е. вызывать ущерб, сопоставимый с последствиями традиционного вооруженного нападения [7; 8]. Во-вторых, ответные меры должны соответствовать принципам необходимости и пропорциональности, т. е. быть необходимыми для защиты и соразмерными нанесенному ущербу [4; 12].

---

[5] *Sanger D. E., Perlroth N.* U.S. Cyberattacks against Iran: escalating online conflict // The New York Times. 2019. June 15. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[6] *Nakashima E.* Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers // The Washington Post. 2019. June 22. URL: https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

Примером практического применения этих принципов является реакция США на кибератаку WannaCry в 2017 г.[7] Обвинив Северную Корею в организации атаки, США предприняли ответные кибермеры[8]. Однако законность таких действий остается предметом дискуссий, учитывая сложности с атрибуцией и оценкой пропорциональности ответных мер [14].

Использование права на самооборону для оправдания наступательных кибероперaций вызывает критику. Нарушение принципов пропорциональности и необходимости может подрывать международные правовые нормы и повышать риск эскалации конфликтов [15]. Кроме того, отсутствие четких соответствующих международных норм и механизмов регулирования усложняет оценку правомерности таких действий [16; 17].

Политико-правовые и доктринальные споры

В рамках Группы правительственных экспертов ООН (GGE)[9] было признано, что международное право применимо к киберпространству. Однако государства не достигли единого мнения относительно квалификации кибератак как акта агрессии или вооруженного нападения [12].

Россия выступает за ограничение применения силы в ответ на кибератаки и за укрепление принципа киберсуверенитета[10]. Российская позиция основана на необходимости разработки новых международных норм, учитывающих специфику киберпространства и предотвращающих эскалацию конфликтов [18].

Соединенные Штаты поддерживают возможность применения права на самооборону в ответ на серьезные кибератаки и считают, что существующие международные нормы могут быть адаптированы к киберпространству [4]. Они акцентируют внимание на необходимости сдерживания и готовности к ответным действиям.

Китай продвигает концепцию киберсуверенитета и государственного контроля над киберпространством[11], выступая за строгий национальный

---

7 The White House (U.S.). Press briefing on the attribution of the WannaCry malware attack to North Korea. URL: https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

8 Department of justice (U.S.). North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. URL: https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and-intrusions.

9 Доклад Группы правительственных экспертов ООН по развитию в области информационно-коммуникационных технологий в контексте международной безопасности. Документ ООН A/68/98, 2013 г. URL: https://undocs.org/A/68/98.

10 МИД России. Позиция Российской Федерации по международной информационной безопасности. 2018. URL: https://www.mid.ru/foreign_policy/information_security/-/asset_publisher/.

11 Cyberspace administration of China (CAC). International strategy of cooperation on cberspace (Международная стратегия Китая по сотрудничеству в кибер-

контроль и против внешнего вмешательства [10; 6]. Китайская позиция подразумевает также необходимость международного сотрудничества для разработки новых норм и правил поведения в киберпространстве.

Не каждое нарушение суверенитета через кибератаку может быть приравнено к применению силы. Проблема атрибуции – точного установления источника кибератаки – усложняет применение права на самооборону [14]. Часто невозможно с полной уверенностью определить, какое именно государство или актор несет ответственность за атаку, что затрудняет принятие правомерных ответных мер[12].

Перспективы кодификации и унификации норм

Одной из ключевых инициатив в области регулирования киберпространства является деятельность Открытой рабочей группы ООН (OEWG), учрежденной Генеральной Ассамблеей ООН в 2018 г.[13] Цель этой группы состоит в разработке общепринятых норм, правил и принципов ответственного поведения государств в киберпространстве. В 2021 году группа опубликовала доклад[14], подтверждающий применимость международного права в киберпространстве и подчеркивающий необходимость международного сотрудничества [15]. Продление мандата группы до 2025 г. свидетельствует о намерении продолжить работу над рекомендациями.

Кроме того, Группа правительственных экспертов ООН (GGE) занимается изучением мер по укреплению безопасности и стабильности в киберпространстве[15]. В докладе 2021 г. GGE[16] подтвердила, что международное право, включая Устав ООН, применимо к киберпространству. Были разработаны добровольные нормы ответственного поведения государств, что является важным шагом на пути к кодификации.

пространстве). URL: https://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

[12] Резолюция Генеральной Ассамблеи ООН 74/247. Противодействие использованию информационно-коммуникационных технологий в преступных целях, 2019 г. URL: https://undocs.org/ru/A/RES/74/247.

[13] Организация Объединенных Наций. Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025). Официальная страница заседаний (UNODA Meetings Place). URL: https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

[14] Организация Объединенных Наций. Итоговый доклад Рабочей группы открытого состава по вопросам развития в сфере информационно-коммуникационных технологий в контексте международной безопасности (2019–2021). A/75/816. Нью-Йорк : ООН, 2021. URL: https://undocs.org/ru/A/75/816.

[15] Организация Объединенных Наций. Доклад Группы правительственных экспертов по достижениям в области информационно-коммуникационных технологий в контексте международной безопасности. Документ ООН A/70/174. Нью-Йорк : ООН, 2015. URL: https://undocs.org/ru/A/70/174.

[16] См.: Документ ООН A/75/816.

Будапештская конвенция о киберпреступности 2001 г.[17] остается единственным действующим международным договором, регулирующим вопросы киберпреступности[18]. В настоящее время ведется работа над Вторым дополнительным протоколом, целью которого является улучшение международного сотрудничества в этой области.

Различные региональные организации также принимают меры для укрепления кибербезопасности. Европейский союз принял Директиву NIS2, направленную на повышение уровня кибербезопасности в Европе [19]. НАТО признает киберпространство как сферу военных операций и работает над развитием киберспособностей своих членов [20].

Несмотря на значительные усилия государств и организаций, существуют серьезные препятствия на пути к унификации норм в киберпространстве. Поляризация позиций государств по вопросам киберсуверенитета и свободы интернета затрудняет достижение консенсуса [10; 15]. Различия в подходах к регулированию киберпространства и недоверие между государствами, вызванное опасениями относительно вмешательства и шпионажа, осложняют международный диалог[19].

Технические сложности, такие как проблема атрибуции кибератак, также препятствуют разработке эффективных правовых механизмов. Без возможности точно установить источник атаки применение международного права и привлечение виновных к ответственности становятся затруднительными[20].

Перспективы развития международного права в области кибербезопасности связаны с продолжением работы международных организаций и укреплением сотрудничества между государствами. Многосторонний подход, включающий партнерство между государствами, частным сектором и гражданским обществом, может способствовать разработке общепринятых норм и стандартов.

Обсуждение и заключение

Применение правовых критериев и международных норм на практике

Национальные стратегии кибербезопасности различных государств демонстрируют разнообразие подходов к применению правовых норм в киберпространстве.

---

[17] Совет Европы. Конвенция о киберпреступности (Будапештская конвенция). Будапешт, 23 ноября 2001 г. ETS No. 185. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[18] Международный комитет Красного Креста. Международное гуманитарное право и кибероперации во время вооруженных конфликтов. Женева : МККК, 2019. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_ru.pdf.

[19] North Atlantic Treaty Organization (NATO). NATO 2022 Strategic Concept (Стратегическая концепция НАТО 2022 г.). Adopted in Madrid, 29 June 2022. Brussels : NATO, 2022. URL: https://www.nato.int/strategic-concept/#download.

[20] См.: Документ ООН A/RES/74/247.

Россия в Доктрине информационной безопасности[21] рассматривает кибератаки, нарушающие суверенитет, как потенциальные акты агрессии, даже если они не приводят к физическому ущербу. Россия подчеркивает необходимость разработки новых международных норм, признающих киберсуверенитет и обеспечивающих национальную безопасность.

Соединенные Штаты Америки квалифицируют серьезные кибератаки на критическую инфраструктуру как применение силы. В Национальной стратегии кибербезопасности 2018 г. США заявляют о готовности применять право на самооборону в ответ на такие угрозы[22]. США считают, что существующие нормы международного права могут быть адаптированы к киберпространству без необходимости разработки новых договоров.

Великобритания признает возможность квалификации кибератак как акта агрессии при наличии значительного ущерба. В Национальной стратегии кибербезопасности 2022 г. подчеркиваются необходимость адаптации существующих норм международного права и важность международного сотрудничества[23].

Китай занимает позицию, согласно которой кибератаки, подрывающие национальные интересы, являются угрозой суверенитету. Китай продвигает концепцию киберсуверенитета и государственного контроля над киберпространством, выступая за создание новых международных норм, признающих право государств на контроль над своими киберсистемами[24].

Различия в подходах затрудняют разработку единых международных норм. Однако практика применения государствами национальных стратегий и участие в международных инициативах демонстрируют стремление найти баланс между национальными интересами и необходимостью глобального регулирования.

Заключение

Проведенный анализ международно-правовых актов и доктрины международного права демонстрирует, что кибератаки могут квалифицироваться как «применение силы» или «акт агрессии», если они вызывают существенный ущерб, сопоставимый с последствиями традиционного вооруженного нападения. Однако отсутствие четких международных норм и различия в

---

[21] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646). URL: https://base.garant.ru/71556224/.

[22] См.: National Cyber Strategy of the United States of America, 2018.

[23] HM Government (United Kingdom). National Cyber Strategy 2022 (Национальная стратегия кибербезопасности 2022 г.). London : HM Government, Dec 2021. URL: https://www.gov.uk/government/publications/national-cyber-strategy-2022.

[24] Ministry of Foreign Affairs of the People's Republic of China. International Strategy of Cooperation on Cyberspace (Международная стратегия сотрудничества Китая в киберпространстве). Beijing, 2017 Mar 1. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3521689/Document-12-Ministry-of-Foreign-Affairs-People-s.pdf.

позициях государств создают значительные трудности в применении права на самооборону в киберпространстве.

Необходимость адаптации международного права к реалиям цифровой эпохи становится все более очевидной. Традиционные нормы, разработанные для регулирования физических вооруженных конфликтов, не всегда эффективно применимы к кибератакам, что требует их переосмысления и обновления. Проблема атрибуции остается одним из ключевых препятствий, поскольку сложности в установлении источника кибератак затрудняют правоприменение и принятие обоснованных ответных мер.

Международное сотрудничество приобретает сущностное значение: только через диалог и совместные усилия возможно разработать унифицированные нормы и механизмы противодействия кибератакам. Различия в национальных подходах подчеркивают важность компромисса и поиска баланса интересов для эффективного регулирования киберпространства.

Рекомендуется инициировать переговоры по созданию международных договоров, учитывающих специфику киберпространства и интересы всех государств. Усиление международного сотрудничества, создание платформ для обмена информацией и проведения совместных расследований помогут повысить эффективность противодействия киберугрозам и уровень доверия между государствами. Признание киберсуверенитета и уважение права государств на контроль над своим киберпространством могут способствовать стабильности и предсказуемости в международных отношениях.

Создание международного механизма атрибуции кибератак, основанного на общепринятых методологиях и стандартах, позволит привлекать виновных к ответственности и снизит риск ошибочных обвинений. Взаимопонимание и сотрудничество государств являются ключевыми факторами в обеспечении безопасности в киберпространстве. Совместными усилиями международное сообщество сможет создать эффективную систему противодействия киберугрозам, обеспечив мир и стабильность в цифровую эпоху.

Список источников

1. Schmitt M. N. Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge : Cambridge University Press, 2017. 569 p.
2. Гаркуша-Божко С. Ю. Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак // Digital Law Journal. 2021. Vol. 2, no. 1. P. 64–82.
3. Zetter K. Countdown to Zero Day: stuxnet and the launch of the world's first digital weapon. New York : Crown, 2015. 448 p.
4. Hathaway O., Crootof R., Levitz P. et al. The law of cyber-attack // California Law Review. 2012. Vol. 100, issue 4. P. 817–885.
5. Горелик И. Б. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта уни-

версальной конвенции // Международное право. 2022. № 4. С. 60–71. DOI: 10.25136/2644-5514.2022.4.39376.

6. Huang Z., Ying Y. The Chinese approach to jus ad bellum in international law and cyberwarfare // The Cambridge Handbook of China and International Law / eds. I. Rasilla, C. Cai. Cambridge : Cambridge University Press, 2024. P. 203–218.
7. Lin H. S. Offensive cyber operations and the use of force // Journal of National Security Law & Policy. 2010. Vol. 4, issue 1. P. 63–86.
8. Roscini M. Cyber operations and the use of force in international law. Oxford : Oxford University Press, 2014. 301 p.
9. Терентьева Л. В. Понятие киберпространства и очерчивание его территориальных контуров // Российский юридический журнал. 2018. № 4. С. 66–71.
10. Jiang C. Decoding China's perspectives on cyber warfare // Chinese Journal of International Law. 2021. Vol. 20, issue 2. P. 257–312. DOI: 10.1093/chinesejil/jmab022.
11. Капустин А. Я. Международное право и вызовы XXI века // Журнал российского права. 2014. № 7. С. 5–19. DOI: 10.12737/4819.
12. Schmitt M. N. Cyber operations in international law: use of force, collective security, self-defense, and armed conflicts // Proceedings of a Workshop on deterring cyberattacks. Washington (DC) : National Academies Press, 2010. P. 151–178. DOI: 10.17226/12997.
13. Waxman M. C. Cyber-attacks and the use of force: back to the future of Article 2(4) // Yale Journal of International Law. 2011. Vol. 36, issue 2. P. 421–459.
14. Deeks A. Defend forward and cyber countermeasures. Hoover institution, national security, technology, and law working group, aegis series paper No. 2004. Stanford : Stanford University, 2020. 26 p.
15. Данельян А. А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261–269.
16. Иванова К. А., Мылтыкбаев М. Ж., Штодина Д. Д. Понятие киберпространства в международном праве // Правоприменение. 2022. Т. 6, № 4. С. 32–44.
17. Shackelford S. J. From nuclear war to net war: analogizing cyber attacks in international law // Berkeley Journal of International Law. 2009. Vol. 25, no. 3. P. 191–250.
18. Ватрушкин А. А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. № 6 (31). С. 78–84.
19. Bradford A. The Brussels effect: how the European Union rules the world. New York : Oxford University Press, 2020. 404 p. DOI: 10.1093/oso/9780190088583.001.0001.

20. Lewis J. A cyber stability, conflict prevention, and capacity building. Washington, D. C. : Center for Strategic and International Studies (CSIS), 2020. 20 p.

References

1. Schmitt, M. N. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press; 2017. 569 p.
2. Garkusha-Bozhko, S. Yu. [International humanitarian law in cyberspace: ratione materiae, ratione temporis and the problem of qualifying cyberattacks]. *Digital Law Journal*. 2021;2(1):25-46. (In Russ.)
3. Zetter, K. Countdown to Zero Day: stuxnet and the launch of the world's first digital weapon. New York: Crown; 2015. 448 p.
4. Hathaway, O., Crootof, R., Levitz, P., et al. The Law of cyber-attack. *California Law Review*. 2012;100(4):817-885.
5. Gorelik, I. B. [Formation of the international legal system for combating cybercrime: from terminology to the draft of a universal convention]. *Mezhdunarodnoe pravo = [International Law]*. 2022;(4):60-71. (In Russ.) DOI:10.25136/2644-5514.2022.4.39376.
6. Huang, Z., Ying, Y. The Chinese approach to jus ad bellum in international law and cyberwarfare. In: I. Rasilla, C. Cai, eds. *The Cambridge Handbook of China and International Law*. Cambridge: Cambridge University Press; 2024. Pp. 203–218.
7. Lin, H. S. Offensive cyber operations and the use of force. *Journal of National Security Law & Policy*. 2010;4(1):63-86.
8. Roscini, M. *Cyber operations and the use of force in international law*. Oxford: Oxford University Press; 2014. 301 p.
9. Terentyeva, L. V. [The concept of cyberspace and outlining its territorial contours]. *Rossijskij yuridicheskij zhurnal = [Russian Legal Journal]*. 2018;(4):66-71. (In Russ.)
10. Jiang, C. Decoding China's perspectives on cyber warfare. *Chinese Journal of International Law*. 2021;20(2):257-312. DOI: 10.1093/chinesejil/jmab022.
11. Kapustin, A. Ya. [International law and the challenges of the 21st century]. *Journal of Russian Law*. 2014;(7):5-19. (In Russ.) DOI: 10.12737/4819.
12. Schmitt, M. N. Cyber operations in international law: use of force, collective security, self-defense, and armed conflicts. In: *Proceedings of a Workshop on deterring cyberattacks*. Washington (DC): National Academies Press; 2010. Pp. 151–178. DOI: 10.17226/12997.
13. Waxman, M. C. Cyber-attacks and the use of force: back to the future of Article 2(4). *Yale Journal of International Law*. 2011;36(2):421-459.
14. Deeks, A. *Defend forward and cyber countermeasures. Hoover institution, national security, technology, and law working group, aegis series paper No. 2004*. Stanford: Stanford University; 2020. 26 p.

15. Danelian, A. A. [International legal regulation of cyberspace]. *Obrazovanie i pravo = [Education and Law].* 2020;(1):261-269. (In Russ.)
16. Ivanova, K. A., Myltkubaev, M. Zh., Shtodina, D. D. The concept of cyberspace in international law. *Law Enforcement Review*. 2022;6(4):32-44. (In Russ.)
17. Shackelford, S. J. From nuclear war to net war: analogizing cyber attacks in international law. *Berkeley Journal of International Law*. 2009;25(3):191-250.
18. Vatrushkin, A. A. [Legal foundations for ensuring cybersecurity of the Russian Federation's critical infrastructure]. *Eurasian Advocacy.* 2017;(6):78-84. (In Russ.)
19. Bradford, A. *The Brussels effect: how the European Union rules the world*. New York: Oxford University Press; 2020. 404 p. DOI: 10.1093/oso/9780190088583.001.0001.
20. Lewis, J. *A cyber stability, conflict prevention, and capacity building*. Washington, D. C. : Center for Strategic and International Studies (CSIS); 2020. 20 p.

Информация об авторе / Information about the author

Лазарь Константин Константинович, аспирант кафедры международного права Дипломатической академии МИД России (Российская Федерация, 119021, Москва, ул. Остоженка, д. 53/2).
Constantin C. Lazari, Postgaduate Studant at the International Law Department, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation (53/2 Ostozhenka St., Moscow, 119021, Russian Federation).

Автор заявляет об отсутствии конфликта интересов.
The author declares no conflict of interest.

Статья поступила в редакцию 28.10.2024; одобрена после рецензирования 09.12.2024; принята к публикации 24.06.2025.
The article was submitted 28.10.2024; approved after reviewing 09.12.2024; accepted for publication 24.06.2025.